



NetScaler with Unified Gateway

Configuring Litmos

Abstract

Configuring Litmos for SSO enables administrators to manage their users using NetScaler.

Contents

- ABSTRACT0
- CONTENTS1
- DISCLAIMER (DOCUMENTATION)2
- PREFACE.....3
- OVERVIEW4
- CONFIGURING LITMOS FOR SINGLE SIGN-ON4
- CONFIGURING NETSCALER FOR SINGLE SIGN-ON10
- TESTING THE CONFIGURATION.....14

Disclaimer (Documentation)

This document is furnished "AS IS." Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix System, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

Citrix Systems, Inc., the Citrix logo, and Citrix Provisioning Services are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Preface

This section provides an overview about the information included in this guide.

Intended Audience

The information in this guide is intended for the System Administrators.

Document Conventions

The following table lists various conventions used in this guide.

Table 1: Document conventions used in this guide

Convention	Description
Bold	Used for names of interface elements (such as names of fields, panes, windows, menus, buttons, dialog boxes) and what the user specifically selects, clicks, presses, or types.
Note	Used to highlight information that is important.

Overview

The Citrix NetScaler application delivery controller (ADC) helps to load balance, accelerate, optimize, and secure enterprise applications.

Litmos provides learning management system with pre-built courses and e-learning solutions. This learning platform enables organizations to provide training anytime, anywhere.

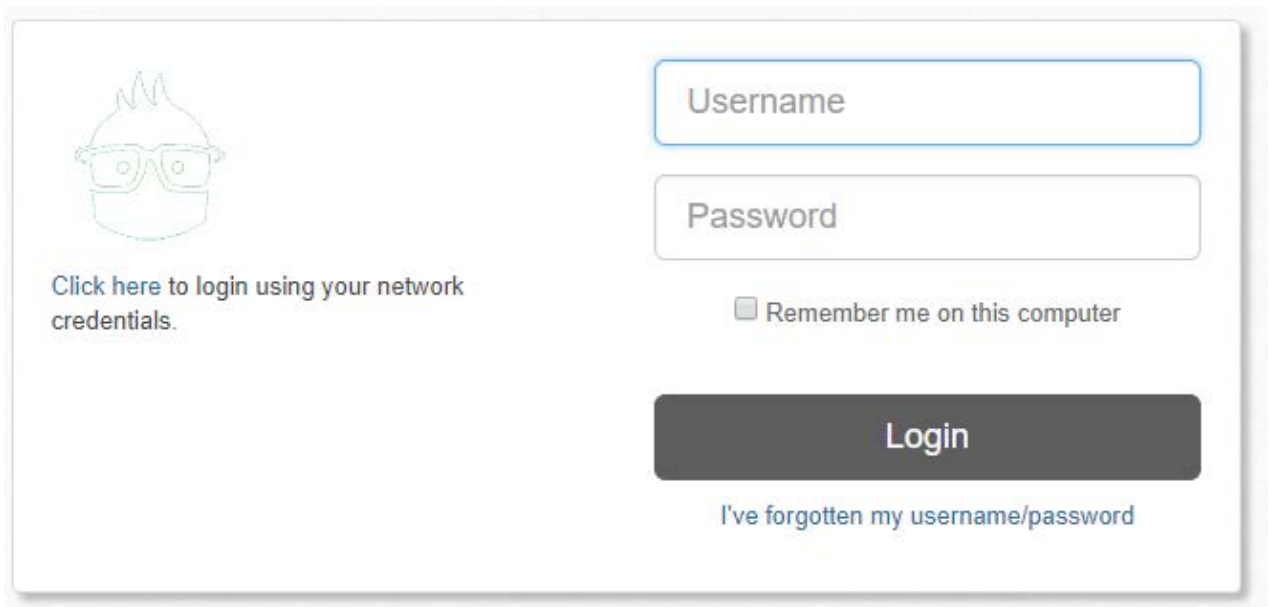
You can connect Litmos with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring Litmos for Single Sign-On

Configuring Litmos for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Litmos using their enterprise credentials.

To configure Litmos for SSO through SAML, follow the steps below:

1. In a browser, type <https://<your-organization>.Litmos.com/> and press enter.
Note: For example, if the URL you use to access pager duty is <https://myserver.Litmos.com>, then you must replace <your-organization> with myserver.
2. Log on to your Litmos account as an administrator.



Click here to login using your network credentials.

Username

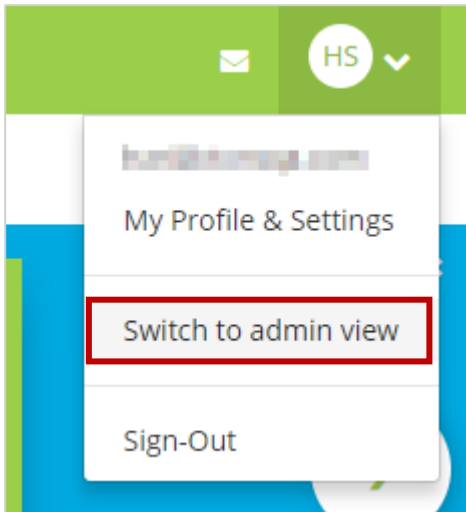
Password

Remember me on this computer

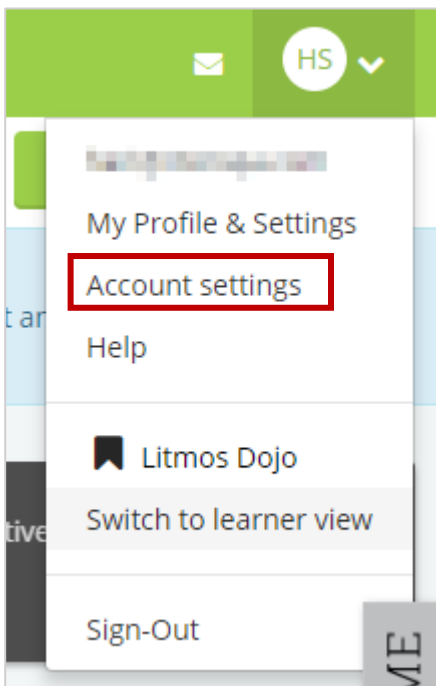
Login

[I've forgotten my username/password](#)

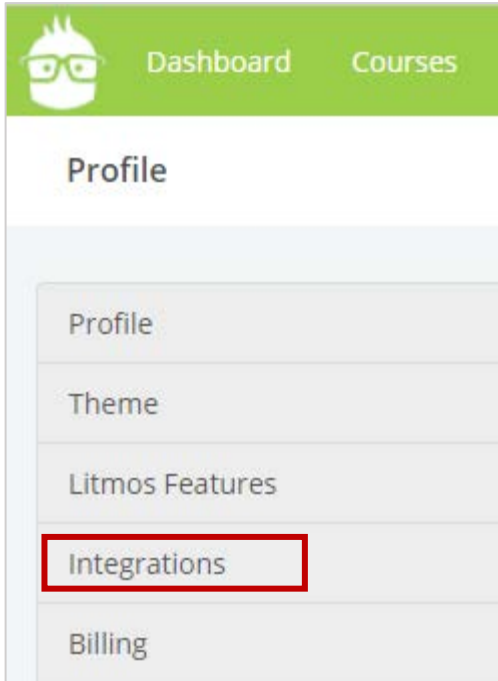
3. On the home page, in the upper right corner, click the profile arrow and click **Switch to admin view**.



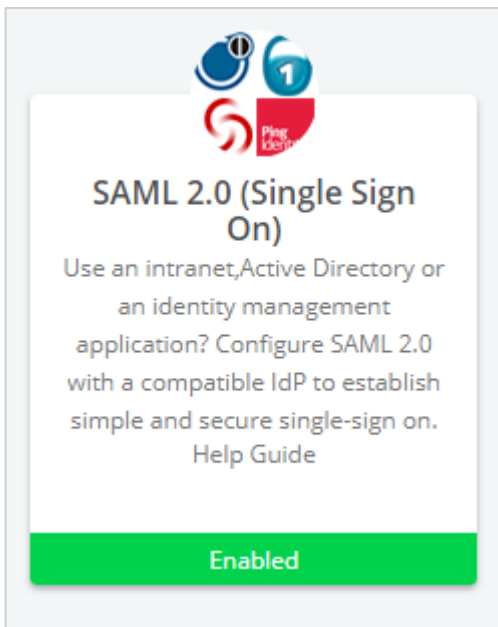
4. After enabling the admin view, in the upper right corner, click the profile arrow and click **Account Settings**.



5. On the **Profile** page, click **Integrations**.



6. On the Litmos Integrations page, click **SAML 2.0 (Single Sign On)**.



7. Click the **Okta and OneLogin users click here** link.

Complete the steps below to configure SAML authentication from your identity provider.

Below are a list of identity providers that support SAML authentication with Litmos:

http://www.okta.com	http://www.onelogin.com
http://www.centify.com	http://www.pingidentity.com
http://azure.microsoft.com	

SAML Metadata

Paste XML Metadata here

Autogenerate Users
(this will automatically create users if they don't exist when logging in)

The SAML endpoint for litmos is:
<https://ctxnsqa.litmos.com/integration/splogin>

Accepted Attributes:
Email, FirstName, LastName

[Okta and OneLogin users click here](#)

Save changes Close

8. Specify the following information for the required fields:

Use an intranet, Active Directory or an identity management application? Configure SAML 2.0 with a compatible IdP to establish simple and secure single-sign on.

Below are a list of identity providers that support SAML authentication with Litmos::

<http://www.okta.com> <http://www.onelogin.com>
<http://www.centrify.com> <http://www.pingidentity.com>
<http://azure.microsoft.com>

Enable SAML 1

Origin URI: 2

SAML x.509 Certificate: 3

```
PA6WlHq80Q5Ll9q7G4nB...RR54F0Z73oL3hotrel+ilU9lo/fda5usH3Qld9OXyV
+-----BEGIN CERTIFICATE-----
MII...
-----END CERTIFICATE-----
```

Autogenerate Users 4
(this will automatically create users if they don't exist when logging in)

The SAML endpoint for litmos is:
[https://\[redacted\].litmos.com/integration/samllogin](https://[redacted].litmos.com/integration/samllogin)

SAML Endpoint for ADFS integrations:
[https://\[redacted\].litmos.com/integration/samllogin?adfs=1](https://[redacted].litmos.com/integration/samllogin?adfs=1)

Accepted Attributes:
Email, FirstName, LastName

5

- i. **Enable SAML**– select the check box.
- ii. **Origin URI** –type your NetScaler FQDN.
- iii. **SAML x.509 Certificate** – This is IdP signing certificate
Click **Browse** to browse to the folder where you saved the IdP provided certificate and upload it.

To obtain your IdP X.509 certificate, follow the steps below:

- i. Remotely access your NetScaler instance using PuTTY.
- ii. Navigate to /nsconfig/ssl folder (using shell command `cd /nsconfig/ssl`) and press Enter.
- iii. Type `cat <certificate-name>` and press Enter.

```
root@pers:~# cd /nsconfig/ssl
root@pers:~/nsconfig/ssl# cat <certificate-name>
-----BEGIN CERTIFICATE-----
MIIC1zCCAkCgAwIBAgIGAWHYpN18MA0GCSqGSIb3DQEEBBQUAMIGuMQswCQYDVOQQGEwJVUzETMBEG
A1I1NDk1MDExMR4wLzE5MDUwLTA1MTUwLTA1MTUwLTA1MTUwLTA1MTUwLTA1MTUwLTA1MTUwLTA1MTUw
FAaWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1
c3R5bGU6IGF1dG8uY29udC5kaW91LnRlc2UuY29udC5kaW91LnRlc2UuY29udC5kaW91LnRlc2UuY29udC5
7aFF3kH99Zhr8i
jPrC4ydcwMxqGdFFSQ/LHWUPGvGlpHzj47MzcN0EbdVmkF61e4/fTkVz3ST3U=
-----END CERTIFICATE-----
root@pers:~/nsconfig/ssl#
```

- iv. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
 - v. Paste the text in a text editor and save the file in an appropriate format such as <your organization name>.pem
- iv. **Autogenerate Users** – select the check box to allow account creation of non-SAML users.
 - v. Click **Save Changes**.

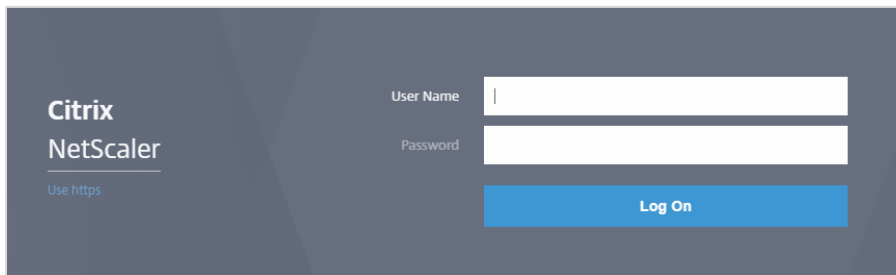
You have completed the required configuration for the service provider which is in this case –Litmos.

Configuring NetScaler for Single Sign-On

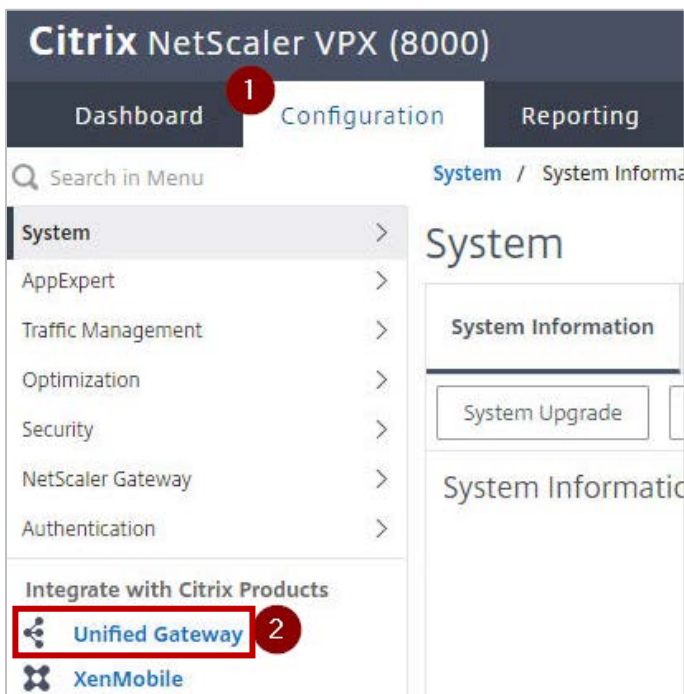
For configuring NetScaler for Litmos, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

To configure NetScaler for single sign on through SAML, complete the following steps:

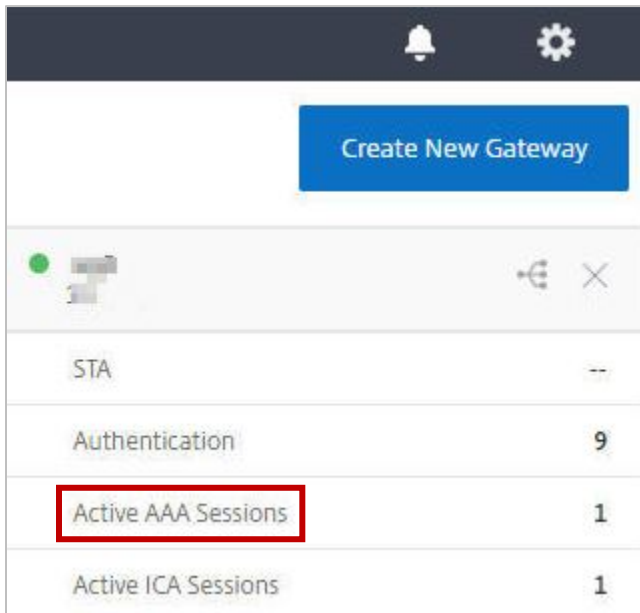
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



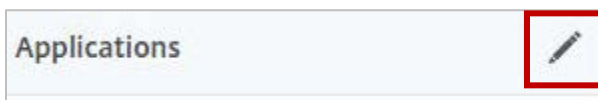
3. Click **Configuration** > **Unified Gateway**.



4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



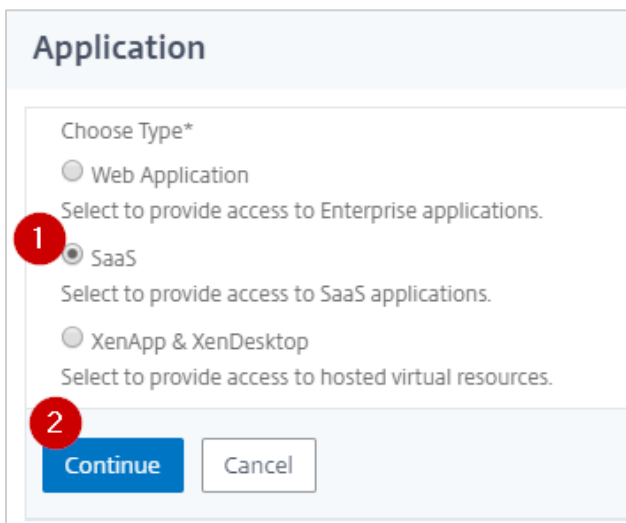
5. Click the edit icon for **Applications** section.



6. For adding a SaaS application, click the plus icon **+** that appears in the edit mode.



7. Click **SaaS > Continue**.



8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Litmos**.

SaaS Application: Catalog vs. Customized

Choose from Catalog Customized Application

Choose from Catalog*

Litmos

Continue Cancel

10. Click **Continue**.
11. In the **Create Application from Template** section, type the name of your SaaS application, in this case Litmos, and relevant comments.

Create Application from Template

Name*

Litmos

Comments

Learning Management System

12. In the subsequent area, specify the following information:

Litmos
by CallidusCloud

Service Provider Login URL*

http://<your-organization>.litmos.cc

Service Provider ID*

Assertion Consumer Service Uri*

https://<your-organization>.litmos.c

Audience

IDP Certificate Name*

Issuer Name

Continue Cancel

- i. **Service Provider Login URL** - type the URL in https://<your-organization>.litmos.com format. **Note:** For example, if the organization's URL is https://myserver.Litmos.com, you must replace <your-organization> with myserver.
- ii. **Service Provider ID** - type the URL in https://<your-organization>.litmos.com format.
- iii. **Assertion Consumer Service Url*** - type the URL displayed by **The SAML endpoint for litmos is** field while configuring Litmos in https://<your-organization>.litmos.com/integration/samllogin format.
Note: For example, if the organization's URL is https://myserver.Litmos.com, you must replace <your-organization> with myserver.
- iv. **Audience** - type the URL that represents service provider in https://<your-organization>.Litmos.com format.
Note: For example, if the organization's URL is https://myserver.Litmos.com, you must replace <your-organization> with myserver.
- v. **IdP Certificate Name** - click the appropriate certificate name.
The IdP certificate appears last in the hierarchy in the **Server Certificate** section on **Unified Gateway Configuration** page.
- vi. **Issuer Name** - type a unique name to identify NetScaler. For example:
MyServer_NS_Litmos

13. Click **Continue**.

14. Click **Done**.

The Litmos logo appears.

15. Click **Done**.

You have completed the NetScaler configuration for Litmos.

Testing the Configuration

Testing the IdP Initiated Flow

To test the IdP initiated configuration, follow the steps below:

1. Access the IdP URL.
2. Log on to NetScaler appliance using your enterprise credentials.
3. Click **Clientless Access**.
4. On the home page, click **Apps** tab.
5. Click **Litmos**.
Your Litmos profile appears.
You have completed testing the IdP initiated flow.



Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2018 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).